



**BEST AVAILABLE COPY**

UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/806,510	04/16/2001	Makoto Saito	010321	9318

43831 7590 08/09/2005

BERKELEY LAW & TECHNOLOGY GROUP  
5250 NE ELAM YOUNG PARKWAY  
SUITE 850  
HILLSBORO, OR 97124

EXAMINER

BAUM, RONALD

ART UNIT PAPER NUMBER

2136

DATE MAILED: 08/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/806,510

Applicant(s)

SAITO, MAKOTO

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 27 May 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 87-178 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 87-178 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- 1) ☐ Certified copies of the priority documents have been received.
  - 2) ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |  |   |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

*pd*

**DETAILED ACTION**

1. This action is in reply to applicant's correspondence of 27 May 2005.
2. Claims 87-178 are pending for examination.
3. Claims 87-178 are rejected.

***Claim Objections***

Claims 12, 13 objection is withdrawn.

Claims 27, 28, 29, 30 objection is withdrawn.

***Claim Rejections - 35 USC § 112***

Claim 30 (and 31-45 by dependency) rejection is withdrawn.

***Double Patenting***

4. Claims 28, 30, 47, 49 (and 31-45, 50-64 by way of dependency) rejection is withdrawn.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Art Unit: 2136

5. Claims 87-178 are rejected under 35 U.S.C. 102(b) as being anticipated by Davis, U.S. Patent 5,825,879.

6. As per claim 87; "A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said method comprising [Abstract, col. 2, lines 10-col. 8, line 51]:

encrypting said decrypted digital data using a changeable key to produce changeable key re-encrypted digital data [i.e., col. 5, lines 5-col. 6, line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' (i.e., changeable) prior to frame buffer storage.];

encrypting said changeable key re-encrypted digital data using an unchangeable key to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied or transferred [col. 6, lines 10-col. 7, line 29, whereas the cryptographic functions in the SVCP IDD portion of the system as broadly interpreted by the examiner clearly encompass both encryption and decryption (i.e., encryption and decryption being the same broad interpretation of encryption per se), and clearly as the SVCP contains digital function, it therefore contains memory storage (i.e., registers, latches, memory, etc; 'storage').];

decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data using said unchangeable key to said changeable key re-encrypted digital data; and

decrypting said changeable key re-encrypted digital data using said changeable key to said decrypted digital data [col. 2, lines 10-col. 8, line 51, whereas the frame buffer encrypted data is clearly decrypted by the reverse procedure insofar as the content becomes rendered on a display.].".

Further, as per claim 102; “An apparatus [This claim is the apparatus claim for the method claim 87 above, and is rejected for the same reasons provided for the claim 87 rejection] for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said apparatus comprising:

a changeable key encryption unit for encrypting said decrypted digital data using a changeable key to produce changeable key re-encrypted digital data;

an unchangeable-key encryption unit for encrypting said changeable-key-re-encrypted digital data using an unchangeable key in a device to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied or transferred;

an unchangeable key decryption unit for decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data using said unchangeable key to said changeable key re-encrypted digital data; and

a changeable key decryption unit for decrypting said changeable key re-encrypted digital data using said changeable key to said decrypted digital data.”.

7. Claim 88 *additionally recites* the limitation that; “A method of claim 87 wherein said unchangeable key may be in a device.”

The teachings of Davis are directed towards such limitations (i.e., col. 3, lines 12-53, col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘ ... key may be in a device ...’

Art Unit: 2136

insofar as the key is used in conjunction with internal data transfer, and is therefore clearly resident in an electronic device.).

Further, as per claim 103; "The apparatus [This claim is the apparatus claim for the method claim 88 above, and is rejected for the same reasons provided for the claim 88 rejection] of claim 102 wherein said unchangeable key may be in a device. "

8. As-per claim 89; "A method for protecting-decrypted-digital-data from illegitimate use, said decrypted digital data being decrypted, from encrypted digital data, comprising [This claim is claim 87 whereas the changeable and unchangeable aspects of the keys are reversed. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed. Therefore this claim is rejected for the same reasons provided for the claim 87 rejection]:

encrypting said decrypted digital data using an unchangeable key to produce unchangeable key re-encrypted digital data;

encrypting said unchangeable key re-encrypted digital data using a changeable key to produce unchangeable-changeable keys double re-encrypted digital data to be stored, copied or transferred;

Art Unit: 2136

decrypting said copied, stored or transferred unchangeable-changeable keys double re-encrypted digital data using said changeable key to said unchangeable key re-encrypted digital data; and

decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data.”.

Further, as per claim 104; “An apparatus [This claim is the apparatus claim for the method claim 89 above, and is rejected for the same reasons provided for the claim 89 rejection] for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from encrypted digital data, said apparatus comprising:

an unchangeable key encryption unit for encrypting said decrypted digital data using an unchangeable key to produce unchangeable key re-encrypted digital data;

a changeable key encryption unit for encrypting said unchangeable key re-encrypted digital data using a changeable key to produce changeable-unchangeable keys double re-encrypted digital data to be stored, copied or transferred;

a changeable key decryption unit for decrypting said copied, stored or transferred changeable-unchangeable keys double re-encrypted digital data using said changeable key to said unchangeable key re-encrypted digital data; and

an unchangeable key decryption unit for decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data.”.

Art Unit: 2136

9. Claim 90 *additionally recites* the limitation that; “A method of claim 89 wherein said unchangeable key may be in a device.

The teachings of Davis are directed towards such limitations (i.e., col. 3, lines 12-53, col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘ ... key may be in a device ... ’ insofar as the key is used in conjunction with internal data transfer, and is therefore clearly resident in an electronic device.).

---

Further, as per claim 105; “The apparatus [This claim is the apparatus claim for the method claim 90 above, and is rejected for the same reasons provided for the claim 90 rejection] of claim 104 wherein said unchangeable key may be in a device. ”

10. Claim 91 *additionally recites* the limitation that; “The method according to claim 87 or 89, wherein said steps of encrypting and decrypting using said changeable key are carried out by a software.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ‘ ... encrypting and decrypting using said changeable key are... carried out by a software’, versus the SVCP per se being either a hardware or software implementation, or more particularly, “The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)”).



Further, as per claim 106 ***additionally reciting*** the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 91 above, and is rejected for the same reasons provided for the claim 91 rejection] according to claim 102 or 104, in which encrypting and decrypting using said changeable key are carried out by a software.”.

11. Claim 92 ***additionally recites*** the limitation that; “The method according to claim 87 or ~~89, wherein said steps of encrypting and decrypting using said changeable key are carried out by~~ a hardware.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ‘ ... encrypting and decrypting using said changeable key are... carried out by a hardware’, versus the SVCP per se being either a hardware or software implementation.).

Further, as per claim 107 ***additionally reciting*** the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 92 above, and is rejected for the same reasons provided for the claim 92 rejection] according to claim 102 or 104, in which encrypting and decrypting using said changeable key are carried out by a hardware.”.

12. Claim 93 ***additionally recites*** the limitation that; “The method according to claim 88 or 90, wherein said changeable key is supplied externally from said device.”.

Art Unit: 2136

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 5-col. 6, line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' (i.e., changeable) prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass '... key is supplied externally from said device ...' insofar as the key is a session key entered externally.).

Further, as per claim 108 *additionally reciting* the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 93 above, and is rejected for the same reasons provided for the claim 93 rejection] according to claim 103 or 105, wherein said changeable key is supplied externally from said device."

13. Claim 94 *additionally recites* the limitation that; "The method according to claim 88 or 90, wherein said changeable key is generated in said device."

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP "... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass '... key is generated in said device ...' insofar as the key is used in conjunction with internal data transfer.).

Further, as per claim 109 *additionally reciting* the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 94 above, and is rejected for the same reasons provided for the claim 94 rejection] according to claim 103 or 105, wherein said changeable key is generated in said device."

14. Claim 95 *additionally recites* the limitation that; “The method according to claim 88 or 90, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ‘ ... encrypting and decrypting using said unchangeable key are... carried out by a software’, versus the SVCP-per-se-being either a hardware or software implementation, or more particularly, “The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)”. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 110 *additionally reciting* the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 95 above, and is rejected for the same reasons provided for the claim 95 rejection] according to claim 102 or 104, in which encrypting and decrypting using said unchangeable key are carried out by a software.”.

Art Unit: 2136

15. Claim 96 ***additionally recites*** the limitation that; “The method according to claim 87 or 89, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ‘ ... encrypting and decrypting using said changeable key are... carried out by a hardware’, versus the SVCP per se being either a

hardware or software implementation. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 111 ***additionally reciting*** the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 96 above, and is rejected for the same reasons provided for the claim 96 rejection] according to claim 102 or 104, in which encrypting and decrypting using said unchangeable key are carried out by a hardware.”.

16. Claim 97 ***additionally recites*** the limitation that; “The method according to claim 88 or 90, wherein said unchangeable key is already placed in said device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly

Art Unit: 2136

interpreted by the examiner would clearly encompass ‘ ... key is already placed in said device ...’ insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an uninitialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 112 *additionally-reciting* the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 97 above, and is rejected for the same reasons provided for the claim 97 rejection] according to claim 103 or 105, wherein said unchangeable key is already placed in said device.”.

17. Claim 98 *additionally recites* the limitation that; “The method according to claim 88 or 90, wherein said unchangeable key is generated in said device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘ ... key is generated in said device ...’ insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an uninitialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 113 ***additionally reciting*** the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 98 above, and is rejected for the same reasons provided for the claim 98 rejection] according to claim 103 or 105, wherein said unchangeable key is generated in said device.”.

18. Claim 99 ***additionally recites*** the limitation that; “The method according to claim 88 or 90, ~~wherein said unchangeable key is supplied externally from said device.~~”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 5-col. 6, line 41, whereas the SVCP clearly re-encrypts with a user/session/ ‘frame data key’ prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass ‘... key is supplied externally from said device ...’ insofar as the key is a session key entered externally. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 114 ***additionally reciting*** the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 99 above, and is rejected for the same reasons provided for the claim 99 rejection] according to claim 103 or 105, wherein said unchangeable key is supplied externally from said device.”.

19. Claim 100 ***additionally recites*** the limitation that; “The method according to claim 88 or 90, wherein said unchangeable key is specific to said device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘ ... key is specific to said device ... ’ insofar as the key is used in conjunction with internal data transfer. Also, the SVCP is applicable to set-top box configurations which inherently have device Ids (i.e., embedded) as part of the processor-PROM/ROM type memory. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 115 ***additionally reciting*** the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 100 above, and is rejected for the same reasons provided for the claim 100 rejection] according to claim 103 or 105, wherein said unchangeable key is specific to said device.”.

20. Claim 101 ***additionally recites*** the limitation that; “The method according to claim 88 or 90, wherein said unchangeable key is not specific to said device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly

Art Unit: 2136

interpreted by the examiner would clearly encompass ‘ ... key is not specific to said device ...’ insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an uninitialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim-116-*additionally-reciting* the limitation that; “The apparatus-[This claim is the apparatus claim for the method claim 101 above, and is rejected for the same reasons provided for the claim 101 rejection] according to claim 103 or 105, wherein said unchangeable key is not specific to said device.”.

21. As per claim 117; “A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising [Abstract, col. 2,lines 10-col. 8,line 51]:

encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data [i.e., col. 5,lines 5-col. 6,line 41, whereas the SVCP clearly re-encrypts with a user/session/ ‘frame data key’ (i.e., changeable) prior to frame buffer storage.];

encrypting said second changeable key re-encrypted digital data using an unchangeable key to produce unchangeable second changeable keys double re-encrypted digital data to be stored [col. 6,lines 10-col. 7,line 29, whereas the cryptographic functions in the SVCP IDD



Art Unit: 2136

portion of the system as broadly interpreted by the examiner clearly encompass both encryption and decryption (i.e., encryption and decryption being the same broad interpretation of encryption per se), and clearly as the SVCP contains digital function, it therefore contains memory storage (i.e., registers, latches, memory, etc; 'storage').];

decrypting said stored unchangeable-second changeable keys double re-encrypted digital data using said unchangeable key to said second changeable key re-encrypted digital data;

encrypting said second changeable key re-encrypted digital data using a third changeable key-to-produce-third changeable-second changeable keys-double-re-encrypted digital data to be copied or transferred [col. 2,lines 10-col. 8,line 51, whereas this is the aspect that deals with the intermediate storage/transfer to intervening memory/storage elements. The SVCP network embodiments clearly encompass this aspect, as broadly interpreted by the examiner.];

decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data using said third changeable key to said second changeable key re-encrypted digital data; and

decrypting said second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data [col. 2,lines 10-col. 8,line 51, whereas the frame buffer encrypted data is clearly decrypted by the reverse procedure insofar as the content becomes rendered on a display.].”.

Further, as per claim 136; “An apparatus [This claim is the method claim for the apparatus claim 117 above, and is rejected for the same reasons provided for the claim 117 rejection] for protecting decrypted digital data from illegitimate use, said decrypted digital data

Art Unit: 2136

being decrypted from digital data encrypted using a first changeable key, said apparatus comprising:

a second changeable key encryption unit for encrypting said decrypted digital data using a second changeable key to produce second changeable key re-encrypted digital data;

an unchangeable key encryption unit for encrypting said second changeable key re-encrypted digital data using an unchangeable key to produce unchangeable-second changeable keys double re-encrypted digital data to be stored;

an unchangeable key decryption unit for decrypting said stored unchangeable-second changeable keys double re-encrypted digital data using said unchangeable key to said second changeable key re-encrypted digital data;

a third changeable key encryption unit for encrypting said second changeable key re-encrypted digital data using a third changeable key to produce third changeable-second changeable keys double re-encrypted digital data to be copied or transferred;

a third changeable key decryption unit for decrypting said copied or transferred third changeable-second changeable keys double re-encrypted digital data using said third changeable key to said second changeable key re-encrypted digital data; and

a second changeable key decryption unit for decrypting said second changeable key re-encrypted digital data using said second changeable key to said decrypted digital data.”.

22. Claim 118 *additionally recites* the limitation that; “The method of claim 117 wherein said unchangeable key may be in a device.”

Art Unit: 2136

The teachings of Davis are directed towards such limitations (i.e., col. 3, lines 12-53, col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘ ... key may be in a device ...’ insofar as the key is used in conjunction with internal data transfer, and is therefore clearly resident in an electronic device.).

Further, as per claim 137; “The apparatus [This claim is the apparatus claim for the method claim 118 above, and is rejected for the same reasons provided for the claim 118 rejection] of claim 136 wherein said unchangeable key may be in a device. ”

23. As per claim 119; “A method for protecting decrypted digital data from illegitimate use, said decrypted digital data being decrypted from digital data encrypted using a first changeable key, said method comprising [This claim is claim 117 whereas the changeable and unchangeable aspects of the keys are reversed. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed. Therefore this claim is rejected for the same reasons provided for the claim 117 rejection]:

encrypting said decrypted digital data using an unchangeable key in a device to produce unchangeable key re-encrypted digital data, and encrypting said unchangeable key re-encrypted

Art Unit: 2136

digital data using a second changeable key to produce second changeable-unchangeable keys double re-encrypted digital data double to be stored;

decrypting said stored second changeable-unchangeable keys double re-encrypted digital data double using said second changeable key to said unchangeable key re-encrypted digital data;

decrypting said unchangeable key re-encrypted digital data using said unchangeable key to said decrypted digital data;

— encrypting said decrypted digital data using a-third-changeable-key to produce third changeable key re-encrypted digital data, and encrypting said third changeable key re-encrypted digital data using said second changeable key to produce second changeable-third changeable keys double re-encrypted digital data to be copied or transferred;

decrypting said copied or transferred second changeable-third changeable keys double re-encrypted digital data using said second changeable key to said third changeable key re-encrypted digital data; and

decrypting said third changeable key re-encrypted digital data using said third changeable key to said decrypted digital data.”.

Further, as per claim 138; this claim is the apparatus claim for the method claim 119 above, and is rejected for the same reasons provided for the claim 119 rejection.

24. Claim 120 *additionally recites* the limitation that; “The method of claim 119 wherein said unchangeable key may be in a device.”

Art Unit: 2136

The teachings of Davis are directed towards such limitations (i.e., col. 3, lines 12-53, col. 5, lines 60-col. 7, line 28, whereas the SVCP “... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘... key may be in a device ...’ insofar as the key is used in conjunction with internal data transfer, and is therefore clearly resident in an electronic device.).

Further, as per claim 139; “The apparatus [This claim is the apparatus claim for the method claim 120 above, and is rejected for the same reasons provided for the claim 120 rejection] of claim 138 wherein said unchangeable key may be in a device.”

25. Claim 121 ***additionally recites*** the limitation that; “The method according to claim 117 or 119, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a software.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ‘... encrypting and decrypting using said changeable key are... carried out by a software’, versus the SVCP per se being either a hardware or software implementation, or more particularly, “The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)”).

Further, as per claim 140 ***additionally reciting*** the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 121 above, and is rejected for the same reasons

Art Unit: 2136

provided for the claim 121 rejection] according to claim 136 or 138, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a software.”.

26. Claim 122 *additionally recites* the limitation that; “The method according to claim 117 or 119, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a hardware.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as-a-digital-computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ‘ ... encrypting and decrypting using said changeable key are... carried out by a hardware’, versus the SVCP per se being either a hardware or software implementation.).

Further, as per claim 141 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 122 above, and is rejected for the same reasons provided for the claim 122 rejection] according to claim 136 or 138, wherein said steps of encrypting and decrypting using said second changeable key are carried out by a hardware.”.

27. Claim 123 *additionally recites* the limitation that; “The method according to claim 118 or 120, wherein said second changeable key is supplied externally from said device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 5-col. 6, line 41, whereas the SVCP clearly re-encrypts with a user/session/ ‘frame data key’ (i.e., changeable) prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass ‘

Art Unit: 2136

... key is supplied externally from said device ...' insofar as the key is a session key entered externally.).

Further, as per claim 142 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 123 above, and is rejected for the same reasons provided for the claim 123 rejection] according to claim 137 or 139, wherein said second changeable key is supplied externally from said device."

---

28. Claim 124 *additionally recites* the limitation that; "The method according to claim 118 or 120, wherein said second changeable key is generated in said device."

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is generated in said device ...' insofar as the key is used in conjunction with internal data transfer.).

Further, as per claim 143 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 124 above, and is rejected for the same reasons provided for the claim 124 rejection] according to claim 137 or 139, wherein said second changeable key is generated in said device."

Art Unit: 2136

29. Claim 125 *additionally recites* the limitation that; “The method according to claim 117 or 119, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a software.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ‘ ... encrypting and decrypting using said changeable key are... carried out by a software’, versus the SVCP per se being either a hardware or software implementation, or more particularly, “The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)”.).

Further, as per claim 144 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 125 above, and is rejected for the same reasons provided for the claim 125 rejection] according to claim 137 or 139, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a software.”.

30. Claim 126 *additionally recites* the limitation that; “The method according to claim 117 or 119, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a hardware.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ‘ ... encrypting and decrypting using said



Art Unit: 2136

changeable key are... carried out by a hardware', versus the SVCP per se being either a hardware or software implementation.).

Further, as per claim 145 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 126 above, and is rejected for the same reasons provided for the claim 126 rejection] according to claim 136 or 138, wherein said steps of encrypting and decrypting using said third changeable key are carried out by a hardware."

---

31. Claim 127 *additionally recites* the limitation that; "The method according to claim 118 or 120, wherein said third changeable key is supplied externally from said device."

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 5-col. 6, line 41, whereas the SVCP clearly re-encrypts with a user/session/ 'frame data key' (i.e., changeable) prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass '... key is supplied externally from said device ...' insofar as the key is a session key entered externally.).

Further, as per claim 146 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 127 above, and is rejected for the same reasons provided for the claim 127 rejection] according to claim 137 or 139, wherein said third changeable key is supplied externally from said device."

Art Unit: 2136

32. Claim 128 *additionally recites* the limitation that; “The method according to claim 118 or 120, wherein said third changeable key is generated in said device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘ ... key is generated in said device ... ’ insofar as the key is used in conjunction with internal data transfer.).

~~Further, as per claim 147 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 128 above, and is rejected for the same reasons provided for the claim 128 rejection] according to claim 137 or 139, wherein said third changeable key is generated in said device.”.~~

33. Claim 129 *additionally recites* the limitation that; “The method according to claim 117 or 119, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ‘ ... encrypting and decrypting using said unchangeable key are... carried out by a software’, versus the SVCP per se being either a hardware or software implementation, or more particularly, “The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)”. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable

Art Unit: 2136

keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 148 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 129 above, and is rejected for the same reasons provided for the claim 129 rejection] according to claim 136 or 138, wherein said steps of encrypting and decrypting using said-unchangeable-key are carried out by a software."

34. Claim 130 *additionally recites* the limitation that; "The method according to claim 117 or 119, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware."

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass '... encrypting and decrypting using said changeable key are... carried out by a hardware', versus the SVCP per se being either a hardware or software implementation. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Art Unit: 2136

Further, as per claim 149 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 130 above, and is rejected for the same reasons provided for the claim 130 rejection] according to claim 136 or 138, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.”.

35. Claim 131 *additionally recites* the limitation that; “The method according to claim 118 or 120, wherein said unchangeable key is already placed in said device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP “... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘... key is already placed in said device ...’ insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an uninitialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 150 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 131 above, and is rejected for the same reasons provided for the claim 131 rejection] according to claim 137 or 139, wherein said unchangeable key is already placed in the device.”.

Art Unit: 2136

36. Claim 132 *additionally recites* the limitation that; “The method according to claim 118 or 120, wherein said unchangeable key is generated in said device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘ ... key is generated in said device ... ’ insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., to-broad-to-be-distinguishable) insofar as any key is inherently changeable from an uninitialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 151 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 132 above, and is rejected for the same reasons provided for the claim 132 rejection] according to claim 137 or 139, wherein said unchangeable key is generated in the device.”.

37. Claim 133 *additionally recites* the limitation that; “The method according to claim 118 or 120, wherein said unchangeable key is supplied externally from said device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 5-col. 6, line 41, whereas the SVCP clearly re-encrypts with a user/session/ ‘frame data key’ prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass ‘ ... key is supplied externally from said device ... ’ insofar as the key is a session key entered externally. The

Art Unit: 2136

examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 152 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 133 above, and is rejected for the same reasons provided for the claim 133 rejection]-according-to-claim 137 or 139, wherein said unchangeable key is supplied externally from the device."

38. Claim 134 *additionally recites* the limitation that; "The method according to claim 118 or 120, wherein said unchangeable key is specific to said device."

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP "... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass '... key is specific to said device ...' insofar as the key is used in conjunction with internal data transfer. Also, the SVCP is applicable to set-top box configurations which inherently have device Ids (i.e., embedded) as part of the processor PROM/ROM type memory. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 153 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 134 above, and is rejected for the same reasons provided for the claim 134 rejection] according to claim 137 or 139, wherein said unchangeable key is specific to said device.”.

39. Claim 135 *additionally recites* the limitation that; “The method according to claim 118 or 120, wherein said unchangeable-key-is-not specific to said device”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP “... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘... key is not specific to said device ...’ insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an uninitialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 154 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 135 above, and is rejected for the same reasons provided for the claim 135 rejection] according to claim 137 or 139, wherein said unchangeable key is not specific to said device.”.

Art Unit: 2136

40. As per claim 155; "A method for protecting digital data from illegitimate use, said method comprising [This claim is claim 87 whereas the changeable and unchangeable aspects of the keys are reversed, and the application specific aspect of licensing (i.e., the 'determining whether said digital data is subject to be protected or not' below). The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an uninitialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed. Also, the SVCP clearly determines protection criteria insofar as the SVCP '... may be necessary to gain prior authorization before viewing of particular video...' (i.e., col. 3, lines 13-26). Therefore this claim is rejected for the same reasons provided for the claim 87 rejection]:

determining whether said digital data is subject to be protected or not;

encrypting said digital data, determined to be protected, using an unchangeable key to produce unchangeable key encrypted digital data;

storing, copying or transferring said unchangeable key encrypted digital data;

decrypting said stored, copied or transferred unchangeable key encrypted digital data using said unchangeable key to said decrypted digital data; and

utilizing said stored, copied or transferred unchangeable key encrypted digital data and said decrypted digital data."

Further, as per claim 167; this claim is the method claim for the apparatus claim 155 above, and is rejected for the same reasons provided for the claim 155 rejection.



41. Claim 156 ***additionally recites*** the limitation that; “The method of claim 155 wherein said unchangeable key may be in a device.”

The teachings of Davis are directed towards such limitations (i.e., col. 3, lines 12-53; col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘ ... key may be in a device ...’ insofar as the key is used in conjunction with internal data transfer, and is therefore clearly resident in an electronic device.).

Further, as per claim 168; “The apparatus [This claim is the apparatus claim for the method claim 156 above, and is rejected for the same reasons provided for the claim 156 rejection] of claim 167 wherein said unchangeable key may be in a device.”

42. Claim 157 ***additionally recites*** the limitation that; “The method according to claim 155, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a software.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass ‘ ... encrypting and decrypting using said unchangeable key are... carried out by a software’, versus the SVCP per se being either a hardware or software implementation, or more particularly, “The SVCP may also be built into equipment such as DVDs and CD ROM devices (both clearly software embodiments per se)”.

Art Unit: 2136

The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 169 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 157 above, and is rejected for the same reasons provided for the claim-157-rejection]-according to claim 167, wherein encrypting-and-decrypting-using said unchangeable key are carried out by a software.".

43. Claim 158 *additionally recites* the limitation that; "The method according to claim 155, wherein said steps of encrypting and decrypting using said unchangeable key are carried out by a hardware.".

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas the SVCP as a digital computer/ processor processing apparatus, as broadly interpreted by the examiner would clearly encompass '... encrypting and decrypting using said changeable key are... carried out by a hardware', versus the SVCP per se being either a hardware or software implementation. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 170 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 158 above, and is rejected for the same reasons provided for the claim 158 rejection] according to claim 167, wherein encrypting and decrypting using said unchangeable key are carried out by a hardware.”.

44. Claim 159 *additionally recites* the limitation that; “The method according to claim 155, in which-encrypting-and decrypting using said unchangeable-key-are-controlled-by identifying information which is added to said digital data.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas, the SVCP clearly determines identifying criteria insofar as the SVCP ‘ ... may be necessary to gain prior authorization before viewing of particular video... ’ (i.e., col. 3, lines 13-26), as broadly interpreted by the examiner would clearly encompass ‘ ... controlled by identifying information ... ’).

Further, as per claim 171 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 159 above, and is rejected for the same reasons provided for the claim 159 rejection] according to claim 167, wherein encrypting and decrypting using said unchangeable key are controlled by identifying information which is added to said digital data.”.

Art Unit: 2136

45. Claim 160 ***additionally recites*** the limitation that; “The method according to claim 159, in which encrypting and decrypting are carried out when said identifying information is present.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas, the SVCP clearly determines identifying criteria insofar as the SVCP ‘ ... may be necessary to gain prior authorization before viewing of particular video... ’ (i.e., col. 3, lines 13-26), as broadly interpreted by the examiner would clearly encompass ‘ ... identifying information is present ... ’).

Further, as per claim 172 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 160 above, and is rejected for the same reasons provided for the claim 160 rejection] according to claim 167, wherein encrypting and decrypting are carried out when said identifying information is present.”.

46. Claim 161 ***additionally recites*** the limitation that; “The method according to claim 159, in which encrypting and decrypting are carried out when said identifying information is absent.”.

The teachings of Davis are directed towards such limitations (i.e., Abstract, col. 2, lines 10-col. 8, line 51, whereas, the SVCP clearly determines identifying criteria insofar as the SVCP ‘ ... may be necessary to gain prior authorization before viewing of particular video... ’ (i.e., col. 3, lines 13-26), as broadly interpreted by the examiner would clearly encompass ‘ ... identifying information is absent ... ’).

Art Unit: 2136

Further, as per claim 173 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 161 above, and is rejected for the same reasons provided for the claim 161 rejection] according to claim 167, wherein encrypting and decrypting are carried out when said identifying information is absent.”.

47. Claim 162 *additionally recites* the limitation that; “The method according to claim 156, wherein said unchangeable key is already placed in said device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP “... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘... key is already placed in said device ...’ insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an uninitialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 174 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 162 above, and is rejected for the same reasons provided for the claim 162 rejection] according to claim 168, wherein said unchangeable key is already placed in the device.”.

Art Unit: 2136

48. Claim 163 *additionally recites* the limitation that; “The method according to claim 156, wherein said unchangeable key is generated in the device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘ ... key is generated in said device ... ’ insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., to-broad-to-be-distinguishable) insofar as any key is inherently-changeable from an uninitialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 175 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 163 above, and is rejected for the same reasons provided for the claim 163 rejection] according to claim 168, wherein said unchangeable key is generated in the device.”.

49. Claim 164 *additionally recites* the limitation that; “The method according to claim 156, wherein said unchangeable key is supplied externally from the device.”.

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 5-col. 6, line 41, whereas the SVCP clearly re-encrypts with a user/session/ ‘frame data key’ prior to frame buffer storage, as broadly interpreted by the examiner would clearly encompass ‘ ... key is supplied externally from said device ... ’ insofar as the key is a session key entered externally. The

Art Unit: 2136

examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 176 additionally reciting the limitation that; "The apparatus [This claim is the apparatus claim for the method claim 164 above, and is rejected for the same reasons provided for the claim 164 rejection]-according-to claim 168, wherein said unchangeable key is supplied externally from the device.".

50. Claim 165 *additionally recites* the limitation that; "The method according to claim 162, 163, or 164, wherein said unchangeable key is specific to the device.".

The teachings of Davis are directed towards such limitations (i.e., col. 5, lines 60-col. 7, line 28, whereas the SVCP " ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ' ... key is specific to said device ...' insofar as the key is used in conjunction with internal data transfer. Also, the SVCP is applicable to set-top box configurations which inherently have device Ids (i.e., embedded) as part of the processor PROM/ROM type memory. The examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to be equivalent (i.e., to broad to be distinguishable) insofar as any key is inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 177 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 165 above, and is rejected for the same reasons provided for the claim 165 rejection] according to claim 174,175 or 176, wherein said unchangeable key is specific to the device.”.

51. Claim 166 *additionally recites* the limitation that; “The method according to claim 162,163 or 164, wherein-said-unchangeable key is not specific to the device.”.\_\_\_\_\_

The teachings of Davis are directed towards such limitations (i.e., col. 5,lines 60-col. 7,line 28, whereas the SVCP “ ... using keys obtained from the encryption circuitry ..., as broadly interpreted by the examiner would clearly encompass ‘ ... key is not specific to said device ...’ insofar as the key is used in conjunction with internal data transfer. The examiner broadly interprets the applicant’s use of the terms changeable and unchangeable keys to be equivalent (i.e., too broad to be distinguishable) insofar as any key is inherently changeable from an uninitialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed.).

Further, as per claim 178 additionally reciting the limitation that; “The apparatus [This claim is the apparatus claim for the method claim 166 above, and is rejected for the same reasons provided for the claim 166 rejection according to claim 174,175 or 176, wherein said unchangeable key is not specific to the device.”.



*Response to Amendment*

52. As per applicant's argument concerning the lack of teaching by Davis of "...using an unchangeable key to produce changeable-unchangeable keys double re-encrypted digital data ...", and "... encrypting said digital data, determined to be protected, using an unchangeable key to produce unchangeable key encrypted digital data ..." the examiner has fully considered in this response to amendment; the arguments, and finds them not to be persuasive. As discussed above, the examiner broadly interprets the applicant's use of the terms changeable and unchangeable keys to-be-equivalent-(i.e., too broad to be distinguishable) insofar-as-any-key-is-inherently changeable from an un-initialized state, and changeability is likewise inherent insofar as upon being initialized, it does not change unless a procedure to change is performed. The Davis teaching of a "frame data keys", downloadable/device transferable public/session key cryptographic information clearly encompasses the applicants "changeable-unchangeable keys" claim elements. Nowhere in the claim language does the recitation of a requirement for an explicit claiming of the differentiation aspect concerning the 2 types of key states appear; just the final state (i.e., changeable-unchangeable) per se. Therefore, the various Davis cryptographic keys, as being *broadly interpreted by the examiner*, as per the claim language, would therefore be applicable in the rejection, such that the rejection support references collectively encompass the said claim limitations in their entirety.

53. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

Art Unit: 2136

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

---

---

Art Unit: 2136

*Conclusion*

54. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner



AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**